

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-239125

(43)Date of publication of application : 31.08.1999

(51)Int.Cl.

H04L 9/08

(21)Application number : 10-040641

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 23.02.1998

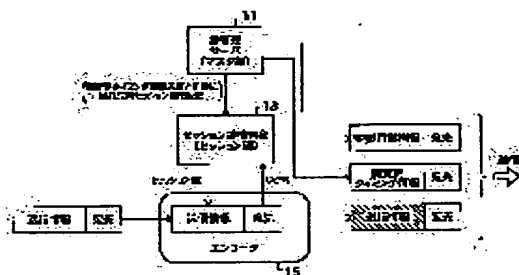
(72)Inventor : KAWABATA MICHIO
NIHEI KATSUTOSHI
NAKAYAMA MASAYOSHI
ARAKI KATSUHIKO

(54) METHOD AND SYSTEM FOR CRYPTOGRAPHIC COMMUNICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To remarkably increase the number of session keys and master keys handleable at an information transmission station by reducing the number of pieces of key information for change by transmitting the session key, which is enciphered by each master key for destination, just for plural destinations.

SOLUTION: When changing the session key, first of all, the destination is turned into destination to change the session key by a key managing server 11 at the information transmission station, a newly generated session key is enciphered by the master key for session key distribution for each destination, and key information for change is generated and transmitted. Afterwards, key application timing information is generated for reporting the application timing of the new session key transmitted by the key information for change to an information reception station and the destination is transmitted as the destination to change the session key. Besides, together with the transmission of key change timing information, the session key for the relevant destination preserved in a session key retrieving part 13 is changed to the new session key.



(19) 日本特許庁 (J P) (12) 公開特許公報 (A) (11) 特許出願公開番号
特開平11-239125
(43) 公開日 平成11年(1998) 8月31日

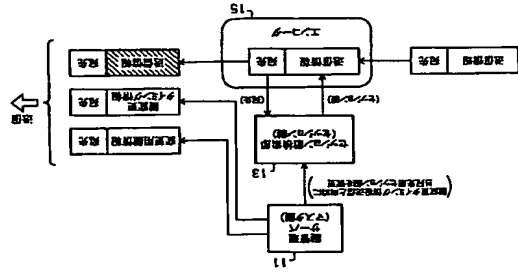
(51) IntCl. ⁴	識別記号	PI
H04L 9/08		H04L 9/00
		601B
		601A
		601E
審査請求 未請求 請求項の数10 O L (全 13 頁)		
(21) 出願番号	特願平10-40841	(71) 出願人 00004228
		日本電信電話株式会社
(22) 出願日	平成10年(1998) 2月23日	東京都新宿区西新宿三丁目19番2号
		川如 道朗
		東京都新宿区西新宿三丁目19番2号 日本
		電信電話株式会社内
		(72) 発明者 仁平 勝利
		東京都新宿区西新宿三丁目19番2号 日本
		電信電話株式会社内
		(72) 発明者 中山 正芳
		東京都新宿区西新宿三丁目19番2号 日本
		電信電話株式会社内
		(74) 代理人 井理士 三好 秀和 (外1名)

(54) 【発明の名称】 暗号化通信方法および暗号化通信システム

(57) 【要約】

【課題】 本発明は、番組単位のみにならず受信局単位の暗号化を可能にすると共に、変更用暗号鍵等の送信数を極力、小さくすることのできる暗号化通信方法および暗号化通信システムを提供することを目的とする。

【解決手段】 情報送信局は、全宛先用のセッション鍵を送信する際に、前記セッション鍵を変更する際に、変更用暗号鍵に複数の宛先に対応するセッション鍵をマスタ鍵で暗号化して送信し、受信局は、前記宛先用のセッション鍵と宛先用マスタ鍵とを保持し、前記伝送情報を受信したときには当該受信局末に記憶されるセッション鍵を用いて当該伝送情報を変換して暗号化して送信する際に、前記変更用暗号鍵を受信する際に前記記憶手段に記憶されるマスタ鍵を用いて復号して変更されたセッション鍵を得る。



知ろうとしても不可能であり、不正復旧はできないようになっている。

【0005】この方法において、番組情報は鍵K_sなどのデスクランブルに必要な情報を持って約1秒に1回送られる。このため、1秒デコーダが番組情報を取り替るとすと、この直後約1秒は鍵K_sがデスクランブルでできなくなってしまう。そこで同じ番組情報を複数回連続送信して受信側で多数決判定できるようにしている。

【0006】また、この方法で用いられるスクランブルアルゴリズムは、映像情報のライン毎に列入れ目を入れ、右を入れ替えるラインローテーション、映像情報のラインを入れ替えるラインバーニャーションなどが用いられている。

【0007】また、CS (Communication satellite) 衛星通信型) デジタル放送では、上記の方法と同様に、鍵構成は3倍で、暗号化はDVB (Digital Video Broadcast) との共通化を図るため、MPEG2 Video & Audio および Systems を単位とした方式を採用している。このため、暗号化はMPEG2 のトランスポートストリームという情報単位で行い、暗号化のアルゴリズムは共通暗号化の1つであるMuller 12 の鍵長32ビット以上の鍵を用いて行っている。この方法では、最大96種類のトランスポートストリームに対し異なる鍵を用いて暗号化を行うことができる。

【0008】また、ATM (Asynchronous Transfer Mode: 非同期伝送モード) を用いた方向通信システムでのセッション鍵の変更が「ATM Forum Technical Committee, Phase 1 ATM Security Specification (Draft), September, 1997」に示されている。このセッション鍵変更法を以下に示す。

【0009】まず、セキュリティ向上のために行うセッション鍵の変更は、各番組用のマスター鍵を各番組の受信資格を持つ全ての受信局に予め与えておく。

【0010】情報送信局でセッション鍵を変更する番組用の新しい鍵を生成し、生成した新しい鍵を当該番組用のマスター鍵で暗号化しセッション鍵送信用のSKE OAM (Operation, Administration, Maintenance: 運用保守) セルに組み込み送信する。この番組の受信資格を持つ各受信局では、当該番組用のSKE OAMセルを受信後、予め与えられたこの番組用マスター鍵で、受信した番組用SKE OAMセルを復号化し、新しいセッション鍵を得る。

【0011】その後、情報送信局は、番組用の鍵変更タイムインジカ通知用のSKE OAMセルを送信すると共に、当該情報送信局における当該番組用のセッション鍵を、SKE OAMセルの送信と同時に、新しいセッション

ン鍵に変更する。また、この番組の受信資格のある全ての受信局で当該番組用のSKE OAMセルを受信すると同時に当該番組用セッション鍵を新しいセッション鍵に変更する。

【0012】
【発明が解決しようとする課題】 上述してきたように、従来の片方向通信暗号化方式は、BS放送用、CS放送用等、複数の受信局で同じ情報を受信する番組毎に異なるセッション鍵及びマスター鍵を持つ暗号化方式である。

【0013】しかしながら、最近では衛星通信等の片方向通信を用いて1受信局に対してのみ情報を送信したいという需要がある。また、ATM Forumに示されているSKE OAMセル及びSKE OAMセルを用いるセッション鍵の変更法は、受信局毎に異なるセッション鍵を用いるシステムに適用する場合には、SKE OAMセル及びSKE OAMセルは各受信局毎に異なるセルを送信する必要があるため、SKE OAMセル及びSKE OAMセルの送信数は受信局の増加に伴い大きく、通信システムの通信帯域に大きな影響を与える。このため、変更用情報及び鍵変更タイムインジカ情報の送信数をできるだけ小さくしたいという課題がある。

【0014】本発明は、上記課題に鑑みてなされたもので、情報送信局で扱うセッション鍵、マスター鍵の数を限定的に小さくすることにより番組単位のマスター鍵局単位での暗号化を可能にすると共に、変更用情報及び鍵変更タイムインジカ情報の送信数を極力、小さくすることのできる暗号化通信方法および暗号化通信システムを提供することを目的とする。

【0015】

【課題を解決するための手段】 前述した目的を達成するために、本発明のうち請求項1記載の発明は、情報送信局で暗号化された所定の鍵が付与された伝送情報を送信し、この伝送情報を当該鍵先の受信端末で受信し復号化するときの暗号化通信方法であって、情報送信局は、全鍵先用のセッション鍵およびマスター鍵とを記憶し、伝送情報を送信するときには当該伝送情報の鍵先に対応するセッション鍵を用いて伝送情報を暗号化して送信し、受信端末は、当該受信端末が受信資格のあるときに限り当てられる鍵先用のセッション鍵と鍵先用マスター鍵とを記憶し、前記伝送情報を受信したときには当該受信端末に記憶されるセッション鍵を用いて当該伝送情報を復号化し、前記セッション鍵を変更する際には、情報送信局は、この情報送信局より送信される変更用情報に鍵先の鍵先に対応するセッション鍵とを記憶し、新しいセッション鍵を、SKE OAMセルの送信と同時に、新しいセッション

マスター鍵で暗号化したものを記憶するものであっても良い。あるいは新規に生成した各鍵先用のセッション鍵を、マスター鍵で暗号化した変更用情報としたものであっても良い。さらにには各鍵先毎に当該鍵先用のマスター鍵で暗号化した複数のセッション鍵を当該変更用情報に記憶するものであっても良く、また複数のセッション鍵をマスター鍵で暗号化したものであっても良い。

【0017】これにより、請求項1記載の本発明では、セッション鍵の変更の際に、情報送信局より送信する変更用情報、複数の鍵先と同時に受信できる変更用情報、情報配送用の鍵先を抑制し、各鍵先用のマスター鍵で暗号化したセッション鍵を複数の鍵先分送信して変更用情報に削減する。

【0018】また請求項2記載の発明は、前記請求項1記載の変更用情報は、各鍵先用の鍵変更タイムインジカ情報と共に送信され、当該鍵変更タイムインジカ情報に従って前記情報送信局および当該鍵先の各情報受信局はセッション鍵を新しいセッション鍵に変更することを要旨とする。

【0019】これにより、請求項3記載の本発明では、セッション鍵の変更の際に、情報送信局より各鍵先用の変更用情報を送信し、各変更用情報で送信した鍵の適用は全鍵先において1つの鍵先用の鍵変更タイムインジカ情報により行い、送信する鍵変更タイムインジカ情報の数を削減する。

【0020】また請求項3記載の発明は、前記請求項1または2記載の情報送信局は、変更用情報及び鍵変更タイムインジカ情報を複数回繰り返して送信することを要旨とする。

【0021】これにより、請求項3記載の本発明では、各情報受信局においてセッション鍵の変更を失敗する確率が小さくなる。

【0022】また請求項4記載の発明は、前記請求項1、2または3記載の情報送信局は複数であることを要旨とする。

【0023】これにより、請求項4記載の本発明では、1つの情報送信局にかかる処理負荷が軽減される。

【0024】また請求項5記載の発明は、前記請求項1乃至4のいずれかに記載のセッション鍵の変更は、変更周期が各鍵先毎に変えて行われることを要旨とする。

【0025】これにより、請求項5記載の本発明では、必要に応じてセッション鍵の変更周期を、安全性と、変更用情報及び鍵変更タイムインジカ情報の送信によるシステムの送信帯域への影響とのトレードオフにより決定する。

【0026】また請求項6記載の発明は、情報送信局で暗号化された所定の鍵が付与された伝送情報を送信し、この伝送情報を当該鍵先の受信端末で受信し復号化するときの暗号化通信システムであって、情報送信局は、全鍵先用のセッション鍵およびマスター鍵とを記憶する

手段と、伝送情報を送信するときには当該伝送情報の鍵先に対応するセッション鍵を用いて伝送情報を暗号化して送信する伝送情報暗号化手段と、前記セッション鍵を変更する際に当該鍵先毎に複数の鍵先に対応するセッション鍵をマスター鍵で暗号化して送信する変更用情報暗号化手段とを有し、受信端末は、当該受信端末が受信資格のあるときに割り当てられる鍵先用のセッション鍵と鍵先用マスター鍵とを記憶する記憶手段と、前記伝送情報を受信したときには当該鍵先毎に記憶されるセッション鍵を用いて当該伝送情報を復号化する伝送情報復号化手段と、前記セッション鍵を変更する際に前記変更用情報を受信して前記記憶手段に記憶されるマスター鍵を用いて復号して変更されたセッション鍵を得る変更用情報復号化手段とを有することを要旨とする。

【0027】これにより、請求項6記載の本発明では、セッション鍵の変更の際に、情報送信局より送信する変更用情報、複数の鍵先で同時に受信できる変更用情報、情報配送用の鍵先を抑制し、各鍵先用のマスター鍵で暗号化したセッション鍵を複数の鍵先分送信して変更用情報に削減する。

【0028】また請求項7記載の発明は、前記請求項6記載の変更用情報は、各鍵先用の鍵変更タイムインジカ情報と共に送信され、当該鍵変更タイムインジカ情報に従って前記情報送信局および当該鍵先の各情報受信局はセッション鍵を新しいセッション鍵に変更することを要旨とする。

【0029】これにより、請求項7記載の本発明では、セッション鍵の変更の際に、情報送信局より各鍵先用の変更用情報を送信し、各変更用情報で送信した鍵の適用は全鍵先において1つの鍵先用の鍵変更タイムインジカ情報により行い、送信する鍵変更タイムインジカ情報の数を削減する。

【0030】また請求項8記載の発明は、前記請求項6または7記載の情報送信局は、変更用情報及び鍵変更タイムインジカ情報を複数回繰り返して送信することを要旨とする。

【0031】これにより、請求項8記載の本発明では、各情報受信局においてセッション鍵の変更を失敗する確率が小さくなる。

【0032】また請求項9記載の発明は、前記請求項6、7または8記載の情報送信局は複数であることを要旨とする。

【0033】これにより、請求項9記載の本発明では、1つの情報送信局にかかる処理負荷が軽減される。

【0034】また請求項10記載の発明は、前記請求項6乃至9のいずれかに記載のセッション鍵の変更は、変更周期が各鍵先毎に変えて行われることを要旨とする。

【0035】これにより、請求項10記載の本発明では、必要に応じてセッション鍵の変更周期を、安全性と、変更用情報及び鍵変更タイムインジカ情報の送信によ

るシステムの送信帯域への影響とのトレードオフにより決定する。

【0036】すなわち、本発明における暗号化通信方法およびこの方法が適用されるシステムでは、情報送信局は、全宛先用のセッション鍵を宛先順に記憶する記憶手段、全宛先用のマスター鍵を宛先順に記憶する記憶手段、

入力情報を記憶する記憶手段を持ち、情報送信局に送信される入力情報と、入力情報の宛先を参照し、参照した宛先が先方のセッションIDの記憶手段より高度に検索し、検索されたセッションIDを用いて、前記入力情報を符号化する符号手段と、セッションIDの変更の際に、各宛先で用いる新しいセッションIDを生成し、当宛先のマスタIDと前記マスタIDの記憶手段より高度に検索し、新しいセッションIDを検索されたマスタIDで呼号化した情報を記憶した変更用記憶手段と、送信する手段と、変更用記憶手段送信後にセッションIDの作成、送信を行うことにより宛先と新しいセッションIDの情報より、当該宛先利用の高度変更タイミング情報を作成、送信すると同時に情報送信局内でのセッションIDの記憶手段の当該宛先利用のセッションIDを新しい宛先IDに変更する手段を備え、受信情報には、受信情報のある宛先利用のセッションIDと、受信情報のある宛先利用のマスタID及び受信情報に添付する記憶手段を持ち、受信側未入力された受信情報宛先の宛先を参照し、参照した宛先利用のセッションIDを受信側未入力のセッションIDの記憶領域より検索し、検索したセッションIDを用いて受信情報を符号化する符号手段と、受信した変更用記憶手段の宛先を参照し、参照した宛先利用のマスタIDを受信情報宛先のマスタIDの記憶領域より検索し、検索したマスタIDを用いて変更用記憶手段の宛先と、受信した変更用記憶手段の宛先を参照し、参照した宛先利用のセッションIDの記憶領域にある当該宛先利用のセッションIDを記憶する手段とを具備する。

【0037】これにより、セッション鍵の変更の際に、情報送信局より送信する各変用暗鍵情報、複数の宛先が同時に宛先でできる変用暗鍵情報配送用の宛先を準備し、各宛先用のマスター鍵で暗号化したセッション鍵を複数の宛先分紅配、送信することにより送信する変用暗鍵の宛先を削減することが可能となる。

【0038】また、セッション鍵の変更の際に、情報送信局より各宛先用の変用暗鍵情報を送信し、各変用暗鍵情報で送信した鍵の適用は宛先において1つの全宛先用の鍵変置タイミング情報により行うことにより、送信する鍵変置タイミング情報の数を削減することが可能となる。

【0039】
【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【0040】図1は本発明の一実施の形態に係る暗号化通信方法が適用される暗号化通信システムの情報送信局

の要部の構成を示すブロック図であり、図2は同、情報受信局の要部の構成を示すブロック図である。図1に示す情報送信局は健康管理サーバ11、セッション鍵発着部13およびエンコーディング部14により構成され、図2に示す情報受信局はセッション鍵出力部2、セッション鍵復着部23およびデコーディング部24により構成される。

【0041】図1に示す情報送信局内のセッション鍵図2では全ての宛先用のセッション鍵を保存しておき、経管制御サーバ11には、全ての宛先利用のセッション鍵と受信局用セッション鍵を保存しているとする。また、図2に示す情報受信局のセッション鍵図25では、情報受信局で受信資格を持つ宛先用の全てのセッション鍵を受信局で受信資格を持つ宛先用の全てのセッション鍵を保存し、セッション鍵抽出部22では当受信局で受信資格を持つ宛先用の全てのマスタ鍵を保存しているものとする。なお、これらセッション鍵とマスタ鍵は図示しないハードディスク、光学的記憶媒体等で構成されるデータベースに蓄積、保存される。

【0042】図1において情報受信局では、パケット形式の情報は宛先情報と承認に送られる伝送情報とから構成される。まず、送信先15に送られる情報として、エンコダがエンコダ15に入力されると、エンコダ15ではパケットの宛先情報と抽出したセッション鍵探索部13に送信し、当該宛先用のセッション鍵を探索し、エンコダ13に送出する。エンコダ13では受け取ったセッション鍵を用いて変復調したパケットの宛先情報を除いた送信情報のみを符号化し、送信する。

【0043】情報受信局においては図2に示すように情報送信局から送られる情報受信局で受信される伝送情報(受信情報)がデコーダ26に入力されると、当該受信情報(受信情報)をデコーダ26に入力されると、当該受信情報(受信情報)を検索し、デコーダ26に送られる。デコーダ26では受け取ったセッション鍵を用いて、受信パケットの宛先情報を除いた受信情報のみを復号化し、出力する。

【0044】 セッション鍵の変更の際には、図1に示す情報送信局の鍵管理サーバ1で、まず宛先を、セッション鍵の変更を行う宛先とし、新しく生成されたセッション鍵を各宛先用のセッション鍵配送用のマスタ鍵で暗号化して宛先用情報群を生成し、送信する。その後、変更用鍵情報で送替した新しいセッション鍵の適用タイミング情報を情報受信局に知らせるための、鍵適用タイミング情報を生成し、宛先をセッション鍵変更を行う宛先とし送信する。また、鍵変更タイミング情報の送信とともにセッション鍵を新しいセッション鍵に更新する。宛先用のセッション鍵を新しくセッション鍵に更新する。

【0045】一方、図2に示す情報受信局では、当該情報受信局で受信資格のある宛先用の変更用情報を受信すると、セッション鍵抽出部22で、予め保存している宛先用のマスター鍵で変更用情報を復号化し新しいセッション鍵を得る。その後、宛先用の鍵変換タイプイン

グ情報を受信すると同時にセッション鍵検索部25に保存している当宛先用のセッション鍵を新しいセッション鍵に変更する。

【0046】図3は、本発明の符号化通信方法が適用される符号化通信システムの1システムを例に、その構成を示すブロック図である。この図3に示す通信システム10を示す。この図3に示す通信システム10は、送信側システム20と受信側システム30とを有する。送信側システム20は、送信側システム20-1から送信側システム20-10を介して受信側システム30へA-TMセル形式で情報を送信する。ここで送信側システム20-10の送信側サーバ11は、センシング側生成部111、マスタ制御部113、SKE OAMセル生成部115およびSKC OAMセル生成部117より構成される。また、受信側システム20は、フィルタ21、センシング側抽出部22、マスタ制御部23、新センシング側抽出部24、マスタ制御部25およびデコード部26よりより構成される。

【0047】まず、送信側システム10のエンコード部15は、情報サーバ1から入力したATMセルのヘッダに含まれる宛先情報であるVPI (Virtual Path Identifier) /VCI (Virtual Channel Identifier) をセッション識別子13へ送信する。セッション識別子13は、全VPI/VCI用のセッション鍵を記憶するようになっている。入力したVPI/VCIを用いたセッション鍵を検索し、該当するセッション/VCIの出力エンコード部16は、セッション識別子13より入力されたセッション鍵を用いてATMセルのペイロードを暗号化し、ペイロードを暗号化したATMセルを出力する。

【0048】受信側システム20のフィルタ21では、入力したATMセルのヘッダに含まれる宛先情報であるVPI/VCIを参照し、当該情報で受信資格であるVPI/VCIに入力したATMセルのヘッダを出力し、それ以外のATMセルは削除する。デコーダ26では、入力したATMセルのヘッダに含まれる宛先情報であるVPI/VCIをセッション識別番号25へ送信する。セッション識別番号25は、当該受信側局20で送信資格のあるVPI/VCI用の鍵のみを記憶できるように構成されており、入力したVPI/VCI用のセッション鍵を検索し、該当するセッション鍵を出力する。

【0049】デコード26は、セッション鍵検索部13より入力されたセッション鍵を用いてATMセルのペイロードを復号化し、ペイロードを復号化したATMセルを出力する。

【0050】セッション鍵の変更は、送信側システム10の鍵管理サーバ11で、セッション鍵の変更を行うV

セルを作成し出力する。その後、出力したSKE OAMセルと同じ宛先VPI/VCIの鍵変更タイミング通知用のSKC OAMセルを作成し、送信すると同時にセッション鍵が更新される当VPI/VCI用セッション鍵を新しいセッション鍵に更新する。

【0051】受信局周シスタム200のセッティング種抽出部22では、SKE OAMセルが入力すると、入力したSKE OAMセルの宛先VPI/VCIをマスタ鍵検索部23に送信する。マスタ鍵検索部23では、VPI/VCI用のマスタ鍵検索表、セッティング種抽出部22へ送信する。セッティング種抽出部22では、マスタ鍵検索部23より受信したマスタ鍵を用いて、受信したSKE OAMセルに含まれる呼号化されたセッション鍵を仮し、当VPI/VCI用の新しいセッション鍵を抽出し、新セッション鍵種抽出部24へ送信する。

【0052】新セッション鍵付機部24ではSKC OAMセルのAMセルの受信と同時に受信したSKC OAMセルの宛先先VPI/VCIを参照し、セッション鍵付索部255に送信し、セッション鍵付索部25は記憶される当VPI/VCI用のセッション鍵を新しいセッション鍵に変更する。

【0053】図4に情報送信局A及び情報受信局A、情報受信局B、情報受信局Cを有するシステムにおけるセッション設定を示す。

【0054】まず、情報送信局Aと情報受信局Aとの変更用超短帯域を作成、送信し、各情報受信局Aにおいては、情報受信局Aのみこの変更用超短帯域を受信する。次に、情報送信局Aと情報受信局Bとの変更用超短帯域を作成、送信し、各情報受信局Bにおいては、情報受信局Bのみこの変更用超短帯域を受信する。次に、情報送信局Aと情報受信局Cとの変更用超短帯域を作成、送信し、各情報受信局Cにおいては、情報受信局Cのみこの変更用超短帯域を受信する。

【0055】次に、情報送信局で情報受信局B宛の変更要用情報を作成、送信し、各情報受信局においては、情報受信受信局Bのみこの変更要用的情報を受信する。次に、情報送信局で情報受信局B宛の追加更変ミミング情報を作成、送信し、各情報受信局においては、情報受信局Bのみこの追加更変ミミング情報を受信し、情報受信局BのセッションIDの変更を完了する。

【0056】最後に、情報送信局で情報受信局Cとの変更に用いた情報を作成、送信し、各情報受信局Cにおいては、情報受信局Cのみこの変更用時間情報を受信する。次に、情報送信局で情報受信局Cとの変更用タイム情報を作成、送信し、各情報受信局Cにおいては、情報受信局Cのみこの変更用タイム情報を受信し、情報受信局Cのセッション間の変更を完了する。

【0057】図5に各変更用情報組に各共用のマスケットで暗号化したセッション鍵を、複数の宛先分記録、送信する場合の、変更用情報組のパケット構成の例を示す。図5に示すパケットでは、情報受信局A、情報受信局B、情報受信局C用の変更用情報組（各宛先用のマスケット）が、情報受信局A、情報受信局B、情報受信局C用の変更用情報組（各宛先用のマスケット）と共に送信される。

タ種で暗号化したセッション鍵)を記載し、宛先として情報受信局Aへ情報受信局Cへの同報用の宛先を用いる。

【0058】この図5に示す変更用鍵情報を用いて、情報送信局、情報受信局A、情報受信局B、情報受信局Cを持つシステムにおいて、セッション鍵の変更を行う際のタイムチャートを図6に示す。

【0059】図6を参照するに、まず情報送信局より、図5に示すA、B、C宛の変更用鍵情報を送信する。各情報受信局A～Cでは、予め変更用鍵情報における各宛先用の変更用鍵情報領域を認識しており、それぞれ受信した変更用鍵情報の該当する領域に認識されている情報を、各情報受信局において予め保持している各宛先用のマスタ鍵で復号化することにより、新しいセッション鍵を得る。

【0060】次に情報送信局で情報受信局A宛の変更用鍵送信情報を作成、送信し、各情報受信局においてタイムミング情報を受信し、各情報受信局Aのセッション鍵の変更を完了する。

【0061】次に、情報送信局で情報受信局B宛の変更用鍵送信情報を作成、送信し、各情報受信局Bにおいてタイムミング情報を受信し、各情報受信局Bのセッション鍵の変更を完了する。

【0062】次に、情報送信局で情報受信局C宛の変更用鍵送信情報を作成、送信し、各情報受信局Cにおいてタイムミング情報を受信し、各情報受信局Cのセッション鍵の変更を完了する。

【0063】図7に1つの変更用鍵情報を複数情報受信局A～情報受信局Cへの同報用の情報受信局として用いる場合の変更用鍵送信情報のパケット構成の一例を示す。図7に示すパケットで宛先として情報受信局Aへ情報受信局Cへの同報用の宛先を用いて、情報送信局で情報受信局A、情報受信局B、情報受信局Cを持つシステムにおいて、セッション鍵の変更を行う際のタイムチャートを図8に示す。

【0064】まず、情報送信局で情報受信局A宛の変更用鍵情報を作成、送信し、各情報受信局においては、情報受信局Aのみこの変更用鍵情報を受信する。次に、情報送信局で情報受信局B宛の変更用鍵情報を作成、送信し、各情報受信局においては、情報受信局Bのみこの変更用鍵情報を受信する。次に、情報送信局で情報受信局C宛の変更用鍵情報を作成、送信し、各情報受信局においては、情報受信局Cのみこの変更用鍵情報を受信する。最後に情報送信局で図7に示す変更用鍵情報を作成、送信し、各情報受信局ではこの変更用鍵情報を受信し、セッション鍵の変更を完了する。

【0065】次に図9及び図10に示すタイムチャートを参照し、変更用鍵情報に記載のセッション鍵を複数回だけ同じセッション鍵を変更用鍵情報として送信する方法の有効性について説明する。図9に、情報送信局よ

り情報受信局Aへ、A宛の変更用鍵情報及びA宛の変更用鍵送信情報を2回ずつ送信し、情報受信局Aにおいて1回目に送信されたA宛の変更用鍵情報を情報受信局Aで受信できなくなった場合のタイムチャートを示している。この場合、1回目に送信されるA宛の変更用鍵情報は情報受信局Aにおいて無効とされ、2回目に送信されるA宛の変更用鍵情報及びA宛の変更用鍵送信情報によりセッション鍵の変更が完了する。

【0066】図10に、情報送信局より情報受信局Aへ、A宛の変更用鍵情報及びA宛の変更用鍵送信情報を2回ずつ送信し、情報受信局Aにおいて1回目に送信されたA宛の変更用鍵送信情報を情報受信局Aで受信できなくなった場合のタイムチャートを示す。この場合、2回目に送信されるA宛の変更用鍵送信情報は無効とし、1回目に送信されたA宛の変更用鍵送信情報と2回目に送信される変更用鍵送信情報によりセッション鍵の変更が完了する。

【0067】図11に本発明を応用した、情報サーバ、情報送信局、情報受信局a、情報受信局b、情報受信局c、情報受信局dを持つシステムの構成の概要を示す。図11の情報送信局dにおいては、情報サーバより入力された、情報受信局aへ情報受信局dへ送信される全ての情報の、暗号化処理を行うことになる。

【0068】これに対して、応用例として、図12に情報サーバ、情報送信局A、情報送信局B、情報受信局a、情報受信局b、情報受信局c、情報受信局dを持つシステムの場合、情報受信局a及び情報受信局Aにおいては、情報サーバより、情報受信局c及び情報受信局d宛に送信される情報の暗号化処理を行い、情報送信局Bにおいては、情報サーバより、情報受信局c及び情報受信局d宛に送信される情報の暗号化処理を行う。このため、図12の情報受信局A及び情報受信局Bでは、図11の情報受信局dでの処理が分散されることになる。

【0069】図13にセッション鍵の変更周期を各宛先宛に変えて行う暗号化通信方法を実現するための情報送信局内の管理サーバの構成の一例を示す。図13に示す管理サーバは、第1の変更用鍵管理110Bが接続されるセッション鍵生成部111と、このセッション鍵生成部111に順次接続されるマスタ鍵検索部113、変更用鍵情報生成部114および変更用鍵送信情報生成部116により構成される。

【0070】第1の変更用鍵管理110Aでは、各受信局宛情報用の宛先のセッション鍵の変更用鍵送信情報(変更用鍵情報及び変更用鍵送信情報)の送信間隔を管理し、例えば10秒毎に第1の変更用鍵送信管理110Aで管理する全ての宛先のセッション鍵の変更を行う。

【0071】また、第2の変更用鍵管理110Bでは複数の受信局宛、番組等の情報用の宛先のセッション鍵

ング情報の個数を減らすことができる。

【0079】また、請求項3および8に記載の暗号化通信方法およびシステムを用いると、情報送信局より各情報受信局へ、変更用鍵情報及び変更用鍵送信情報を複数回送信することから、各情報受信局において、変更用鍵情報及び変更用鍵送信情報の受信失敗の間に、再送される変更用鍵情報及び変更用鍵送信情報によりセッション鍵の変更を完了させることができるため、各情報受信局においてセッション鍵の変更を失敗する確率が小さくなる。

【0080】請求項4および9に記載の暗号化通信方法およびシステムを用いると、情報送信局が複数であることから、1つの情報送信局にかかる処理負荷が軽減される。

【0081】請求項5および10に記載の暗号化通信方法およびシステムを用いると、セッション鍵の変更周期を宛先毎に変えることができ、必要に応じてセッション鍵の変更周期を、安全性と、変更用鍵情報及び変更用鍵送信情報の送信によるシステム全体の送信帯域への影響とのトレードオフにより決定することができる。

【図面の簡単な説明】

【図1】本発明に係る通信システムにおける情報送信局の一実施形態の概略の構成を示すブロック図である。

【図2】本発明に係る通信システムにおける情報受信局の一実施形態の概略の構成を示すブロック図である。

【図3】本発明に係る通信システム全体の概略の構成を示すブロック図である。

【図4】セッション鍵変更法を用いる場合の情報送信局と情報受信局との間のタイムチャートである。

【図5】図1に示す情報送信局から送信される変更用鍵情報の構成例を示す図である。

【図6】図3に示す通信システムで用いられるセッション鍵変更法における情報送信局と情報受信局間のタイムチャートである。

【図7】他の変更用鍵送信情報の構成例を示す図である。

【図8】他の通信システムで用いられるセッション鍵変更法における情報送信局と情報受信局間のタイムチャートである。

【図9】1回目に送信された変更用鍵送信情報が情報受信局で正しく受信できなかった場合のタイムチャートである。

【図10】1回目に送信された変更用鍵送信情報が情報受信局で正しく受信できなかった場合のタイムチャートである。

【図11】本発明が適用される一般的な通信システムの構成を示すブロック図である。

【図12】他の通信システムの構成を示すブロック図である。

【図13】宛先毎にセッション鍵の変更周期を変え方

の変更用鍵情報(変更用鍵情報及び変更用鍵送信情報の送信間隔)を管理し、例えば5秒毎に第2の変更用鍵管理110Bで管理する全ての宛先のセッション鍵の変更を行う。

【0072】これにより、各情報受信局では、各情報受信局用の変更用鍵情報及び変更用鍵送信情報は10秒毎に受信されることにより、各情報受信局宛情報用のセッション鍵は10秒毎に変更される。また、複数の受信局宛の、番組等の情報用の変更用鍵情報及び変更用鍵送信情報は5秒毎に受信することにより、複数の受信局宛の、番組等の情報の宛先用のセッション鍵は5秒毎に変更される。このように目的に合わせてセッション鍵の変更周期を各宛先毎に変えることができる。

【0073】図14に図13に示す情報送信局内の管理サーバを持つことにより、情報受信局A及び情報受信局B用の宛先のセッション鍵の変更を10秒毎に、情報受信局A及び情報受信局Bで受信資格を持つ番組1の宛先用のセッション鍵の変更を5秒毎に行うときの情報送信局と各情報受信局間のタイムチャートを示す。

【0074】図14を参照するに、番組1用の変更用鍵情報及び変更用鍵送信情報の送信、A宛の変更用鍵情報及び変更用鍵送信情報の送信、B宛の変更用鍵情報及び変更用鍵送信情報の送信をまず行う。

【0075】そして約5秒後に番組1用の変更用鍵情報及び変更用鍵送信情報の送信、更に約5秒後に番組1用の変更用鍵情報及び変更用鍵送信情報の送信、A宛の変更用鍵情報及び変更用鍵送信情報の送信、B宛の変更用鍵情報及び変更用鍵送信情報の送信をまず行う。このように情報送信局内で宛先毎にセッション鍵の変更周期を変更することができる。

【0076】尚、上記の実施形態ではATMに適用した場合を例にとり説明したが、本発明はこれに限定されることなく、いかなる形式のパケットを暗号化する暗号化通信システムにおいても、またいかなる暗号化アルゴリズムを用いる暗号化通信システムにおいても、またいかなるセッション鍵の変更周期をもつ暗号化通信システムにおいても適用できる。

【0077】

【発明の効果】上述したように本発明の請求項1および6に記載の暗号化通信方法およびシステムによれば、各変更用鍵情報に各宛先用のマスタ鍵で暗号化したセッション鍵を複数の宛先分配を作成、送信するので、各宛先毎に異なる変更用鍵情報を作成、送信する場合に比べ、送信する変更用鍵情報の個数を減らすことができる。

【0078】また、請求項2および7に記載の暗号化通信方法およびシステムを用いると、情報送信局より各宛先毎に変更用鍵情報を送信し、送信した各変更用鍵情報に記載のセッション鍵の適用を各宛先用の変更用鍵送信情報1つで行うため、各宛先毎に異なる暗号化タイムミング情報を送信する場合に比べ送信する変更用鍵送信

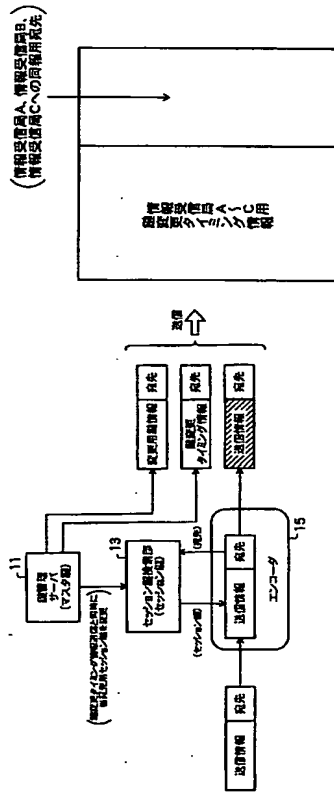
法を実現するための情報送信局内の鍵管理サービスの構成を示すブロック図である。

【図14】宛先毎にセッション鍵の変更周期を変える方法を適用した情報送信局と情報受信局間のタイムチャートである。

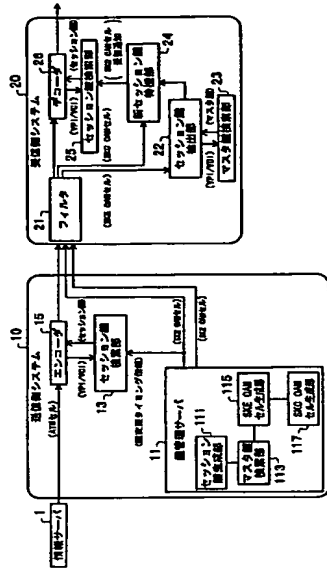
【図15】衛星放送で用いられるスクランブル方法の3重鍵暗号の概要を示す図である。

【符号の説明】

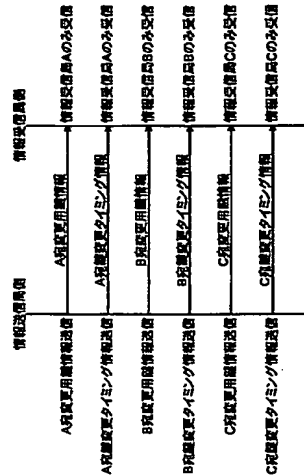
- | | | | |
|----|-----------|-----|--------------|
| 1 | 情報サーバ | 111 | セッション生成部 |
| 10 | 送信側システム | 113 | マスタ検査部 |
| 11 | 健康管理サーバ | 115 | SKE OAMセル生成部 |
| 13 | セッション/検査部 | 117 | SKC OAMセル生成部 |



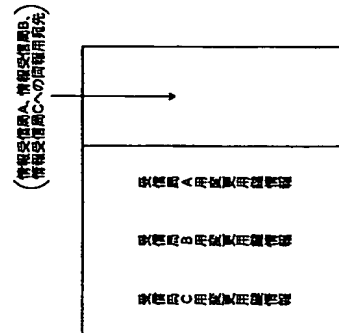
【图7】



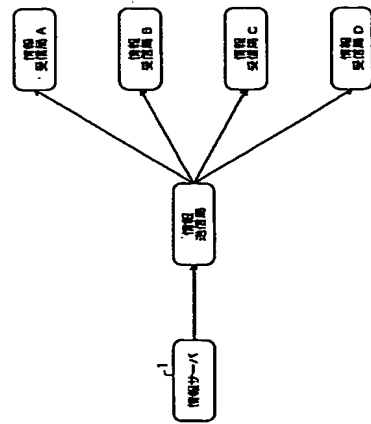
【图4】



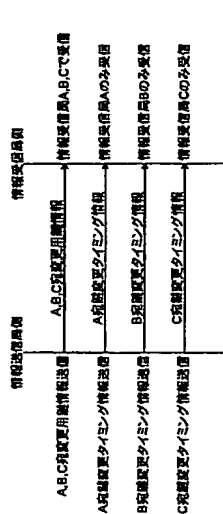
【5】



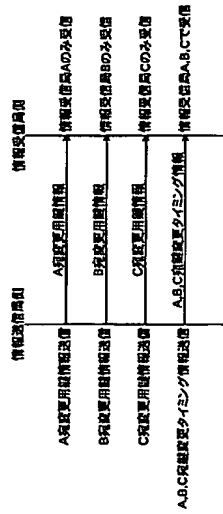
【圖 11】



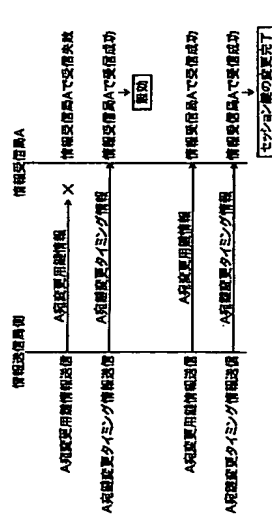
【図6】



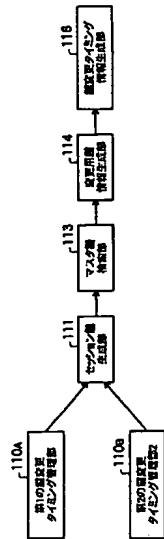
【図8】



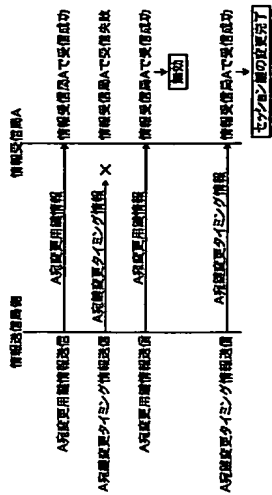
【図9】



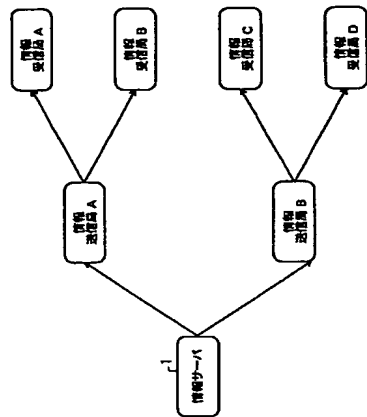
【図13】



【図10】



【図12】



【図15】

